Technical Cybersecurity

The Cyber Killchain

How general is this pattern attacks seem to follow?

The Cyber Killchain

Developed at Lockheed Martin

- Eric Hutchins
- Micheal Cloppert
- Rohan Amin

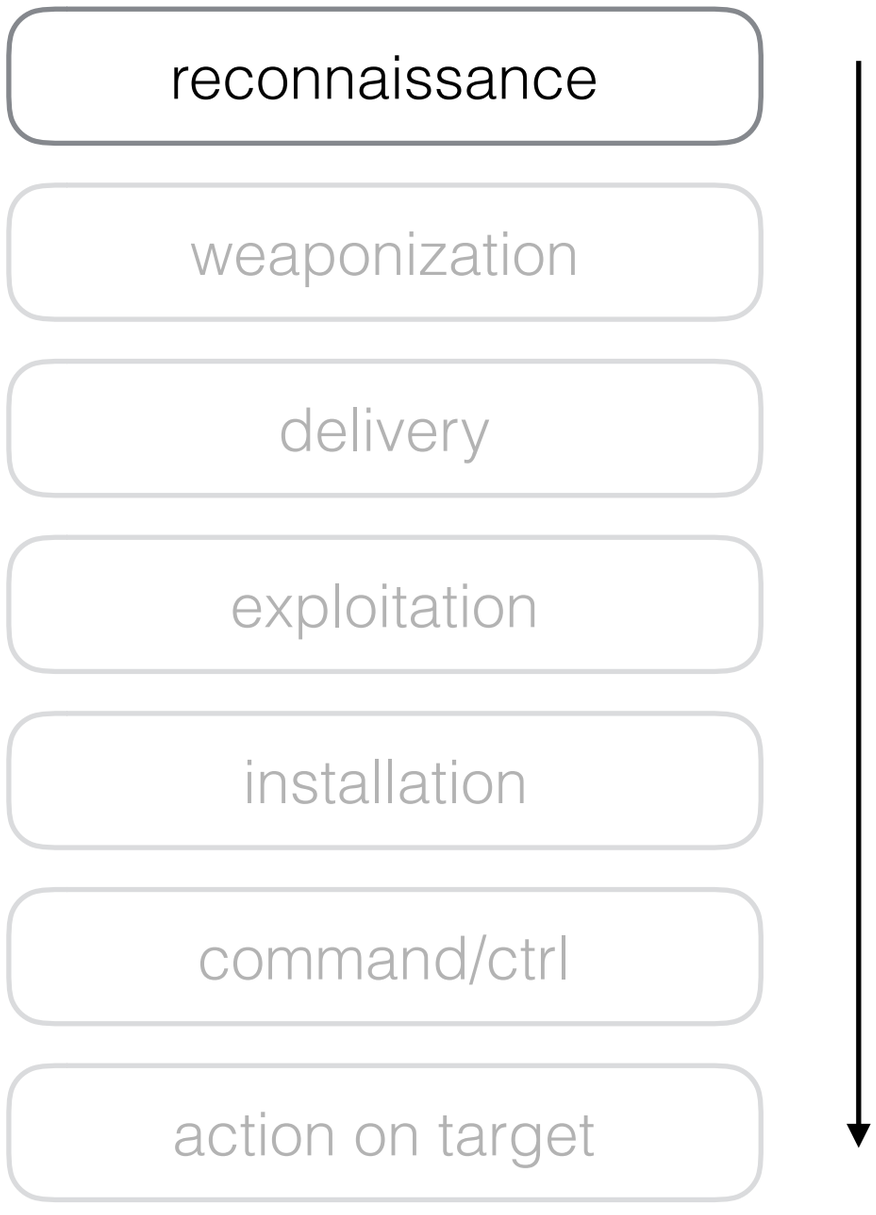
Implemented in Steps

- Model things attacker might do

The Cyber Killchain

We need to know where we are.

It's very important when you first compromise a system to learn everything you can about that system and the systems surrounding it.



The Cyber Killchain

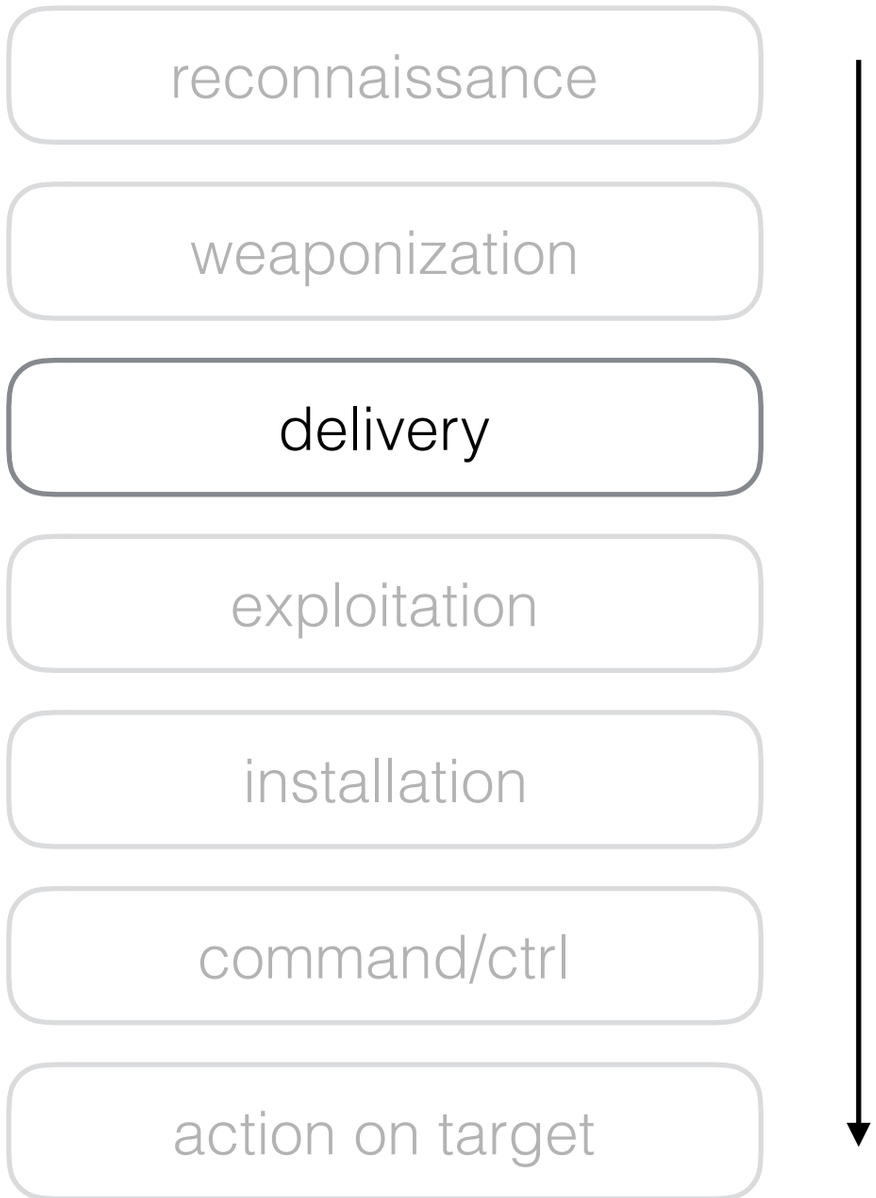
We need to continue the attack.

After the initial compromise, we need to further compromise other systems to gain persistence and to acquire valuable information.

The Cyber Killchain

We need to deliver the payload.

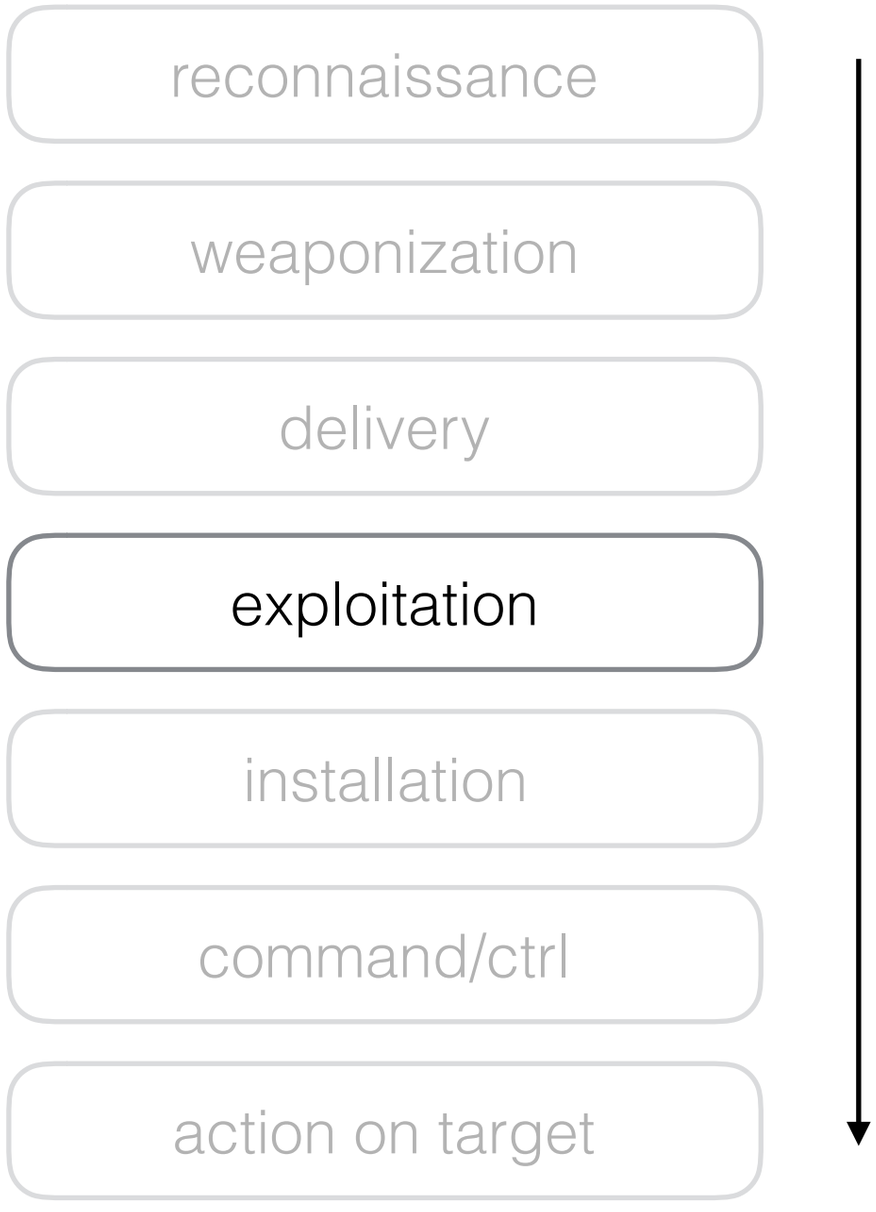
Once we've developed an appropriate exploit to further our compromise, we need to deliver it to vulnerable systems where it'll be invoked.



The Cyber Killchain

We need to execute the exploit.

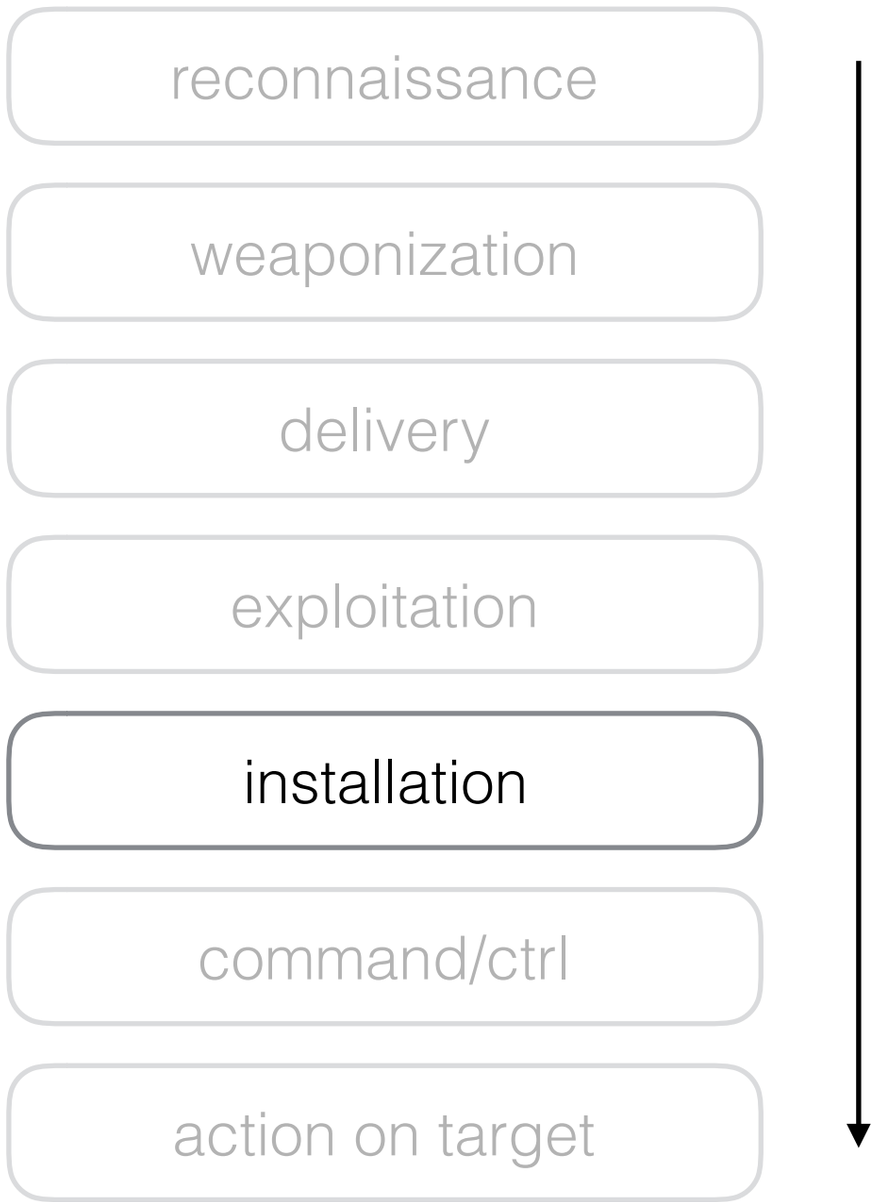
At this point, we have information on the target, and we have a payload that incorporates an exploit that we can use to compromise a system. We need to get that exploit executed.



The Cyber Killchain

We need to install our software.

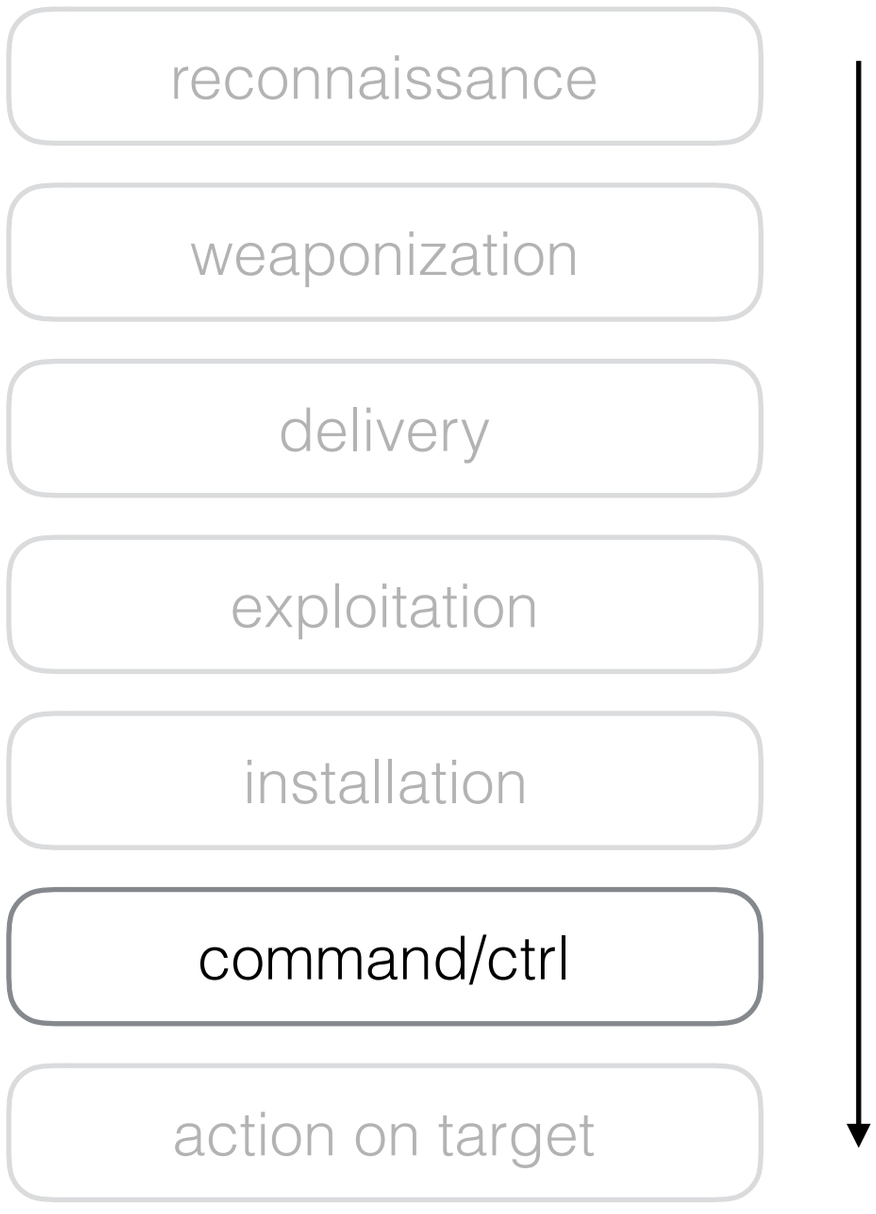
We have exploited the system and have code execution. Now, we need to get our software installed. Usually, the initial exploit runs some small section of code that we deliver, but we want to get more on the system. This can be multi-stage.



The Cyber Killchain

We want to control the host.

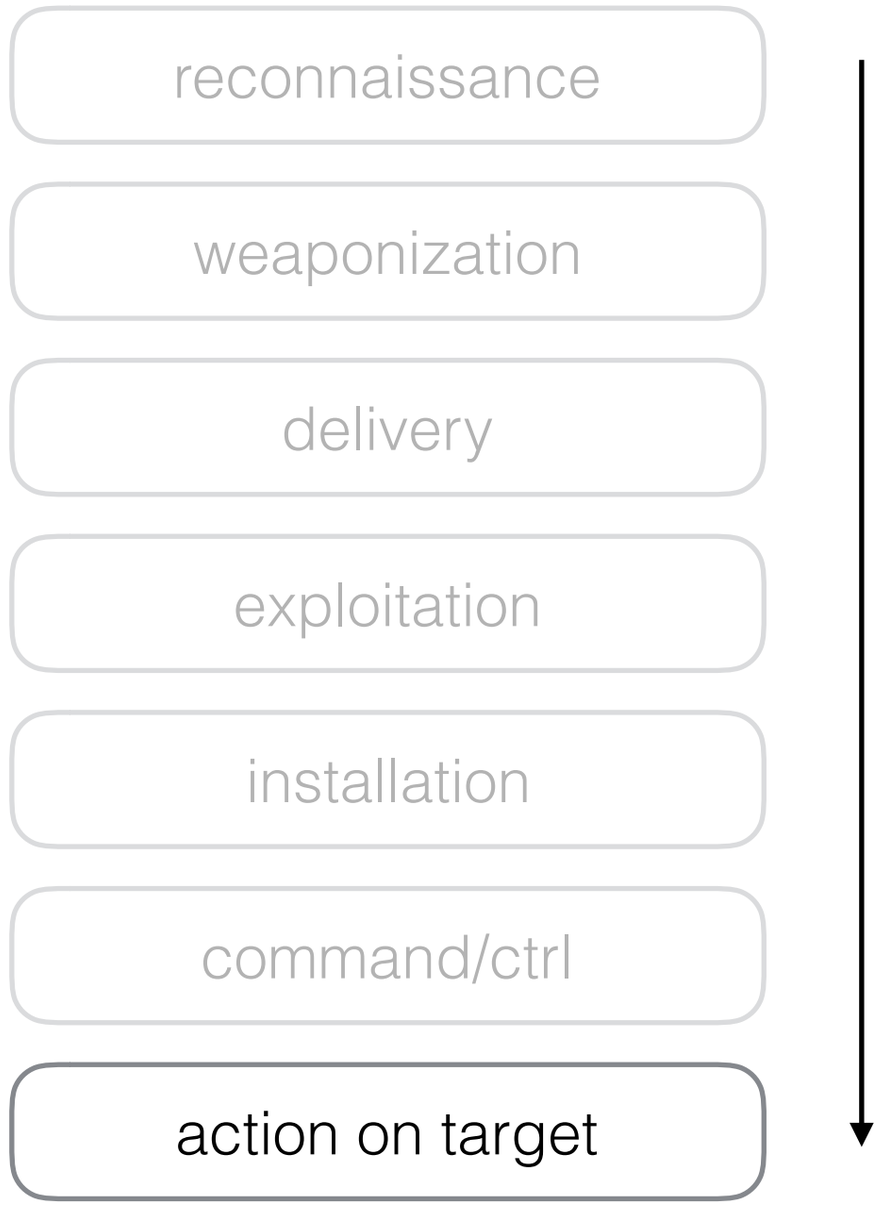
Usually, after the first compromise, we want to control the host. This involves communicating to some kind of backend infrastructure.



The Cyber Killchain

We want to do something!

Usually, we want to take some kind of action on the target we've spend so much time compromising. That could involve exfiltrating data, disrupting systems, or altering information, or really just about anything.



The Cyber Killchain

Sequencing

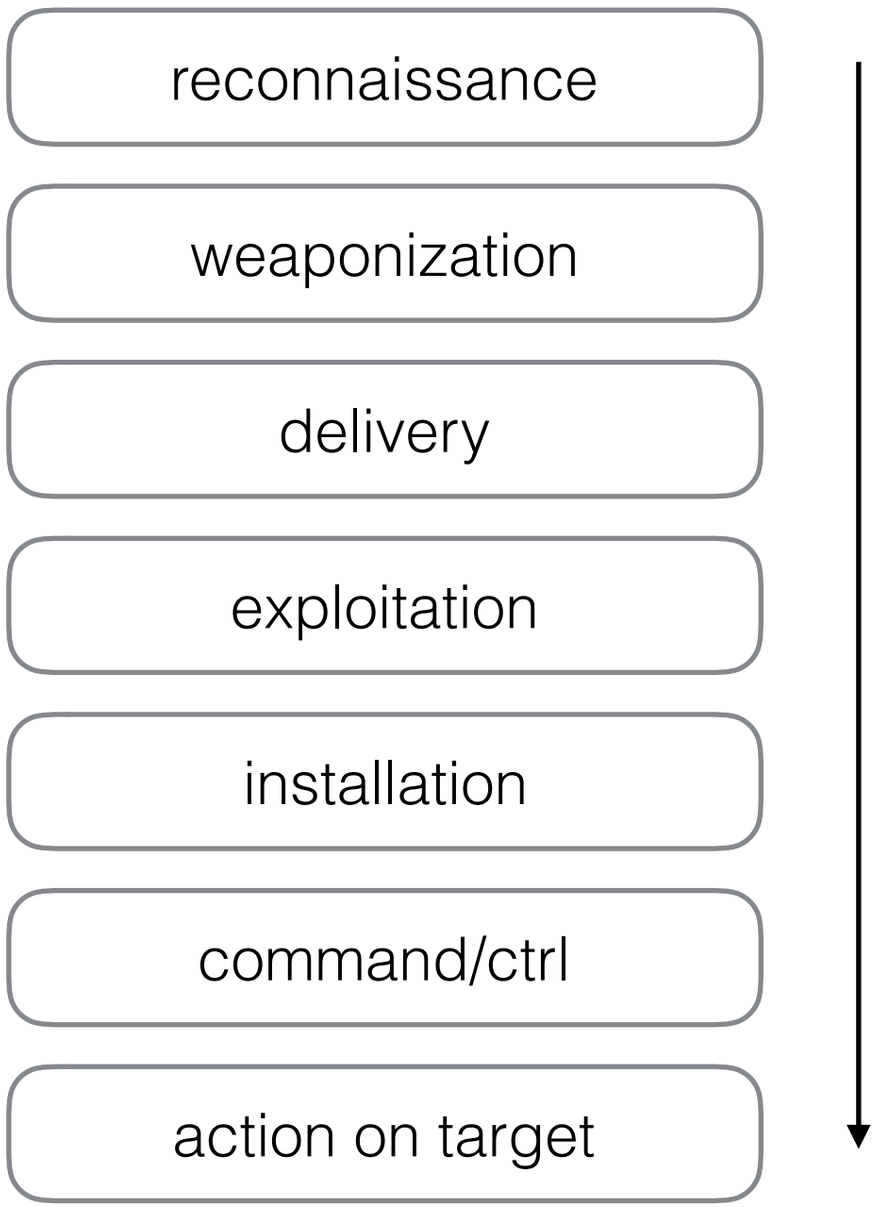
- Not always in sequence
- Frequently start chain over in campaigns

Disruption

- Can we go from one stage to the next if a control is in place?

Location

- Do all campaigns follow this?



How does the Cyber Killchain map to IoT?